

IN THE CLAIMS:

Claims 1-24 (Canceled).

Claim 25 (Currently Amended): A multi-level secure network having a plurality of host computers accessible to users and connected to a network medium that has access to an untrusted line, the secure network comprising:

a network security controller for generating a plurality of user profiles for a single user identifier that a user inputs to allow access to the network and for sending one of said plurality of user profiles as selected by associated with the user identifier to security devices connected to the network medium, each of said user profiles defining at least one of a plurality of destinations which the user is authorized to access through discretionary access control and mandatory access control security mechanisms, wherein a plurality of user profiles define virtual private networks of communication comprising subsets of host computers; and,

security devices connected to the network medium for receiving the said plurality of user profiles, associated with the single user identifier, generated at the network security controller as selected by the user and for implementing security mechanisms associated with the user profiles, each security device associated with one host computer, each security device having an authorization device for authorizing users user identifiers at the associated host computer as inputted by a user, the security device permitting the authorized user, via the associated host computer, to select one of said plurality of user profiles associated with the user identifier and for restricting access of the host computer to the destinations defined in the selected user's profile.

Claim 26 (Original): The network of claim 25, wherein the at least one destination comprises at least one other host computer of the network or the untrusted line.

Claim 27 (Previously Amended): The network of claim 25, wherein the security device, when implementing security mechanisms, allows the host computer to connect to a trusted destination.

Claim 28 (Currently Amended): The network of claim 25, wherein the security device, when not implementing security mechanisms, allows the host computer to connect to an untrusted destination.

Claim 29 (Original): The network of claim 25, wherein the untrusted line comprises the Internet.

Claim 30 (Original): The network of claim 25, wherein a user cannot simultaneously communicate with a trusted destination and an untrusted destination.

Claim 31 (Original): The network of claim 25, wherein a user is prevented from simultaneously connecting to destinations having different security levels.

Claim 32 (Original): The network of claim 25, wherein a user can only select one profile at a time.

Claim 33 (Canceled)

Claim 34 (Original): The network of claim 25, wherein security is implemented at a network layer of protocol hierarchy.

Claims 35 - 36 (Cancelled)

Claim 37 (Original): The network of claim 25, wherein the security devices are integrated with the associated host computer.

Claim 38 (Currently Amended): A method for operating a multi-level secure network having a plurality of host computers accessible to users through input of a single user identifier and a network security controller, each of which are connected to a network medium that has access to an untrusted line, the method comprising:

generating at the network security controller a plurality of user profiles for each user identifier inputted by a user, each of said user profiles defining at least one of multiple destinations which the user is authorized to access through discretionary access control and mandatory access control security mechanisms, to define virtual private networks of communication comprising subsets of host computers;

authorizing a user identifier that a user inputs at a host computer;
permitting, at the host computer, the authorized user to select one of said plurality of user profiles associated with the user identifier;

sending one of said plurality of user profiles from said network security controller, as selected by the authorized user, to said host computer; and

restricting access of the host computer to the destinations defined in the selected user's profile.

Claim 39 (Previously Amended): The method of claim 38, wherein each of the destinations comprise other host computers of the network or the untrusted line.

Claim 40 (Previously Amended): The method of claim 38, further comprising the step of implementing a security mechanism to enable the host computer to connect to a trusted destination.

Claim 41 (Original): The method of claim 38, further comprising the step of not implementing security mechanisms when the host computer connects to an untrusted destination.

Claim 42 (Original): The method of claim 38, wherein the untrusted line comprises the Internet.

Claim 43 (Original): The method of claim 38, wherein a user cannot simultaneously communicate with a trusted destination and an untrusted destination.

Claim 44 (Original): The method of claim 38, wherein a user is prevented from simultaneously connecting to destinations having different security levels.

Claim 45 (Original): The method of claim 38, wherein a user can only select one profile at a time.

Claim 46 (Cancelled)

Claim 47 (Original): The method of claim 38, wherein security is implemented at a network layer of protocol hierarchy.

Claim 48 (Cancelled)

Claim 49 (Original): The method of claim 38, wherein the destination in a user's profile correspond to a level of security granted the user.

Claims 50 - 53 (Cancelled)

Claim 54 (Currently Amended): A multi-level secure network having a plurality of host computers accessible to users and interconnected with the Internet, each user having a user identifier for accessing the secure network, the secure network comprising:

a network security controller for enabling a security officer to generate a plurality of user profiles for at least one of a plurality of user~~user~~ identifiers that a user inputs to access the network, each user profile defining at least one destination from a multiplicity of destinations which a user is authorized to access, and for sending a user profile to a security device, as selected by an authorized user; and,

security devices connected with said host computers for receiving from the security officer the user profiles generated at the network security controller, each security device associated with one host computer, each security device having an authorization system for authorizing users based on a single user

identifier for each user at the associated host computer, the security device permitting the authorized user, via the associated host computer, to select one of the plurality of user profiles associated with the user identifier and for restricting access of the host computer to the destinations defined in the selected user's profile, and wherein each security device includes a communication control system to control access of the host computer to the communication medium, said communication control system including a data storage device for storing data provided by said host computer in a memory space, and for transferring data out of said memory space while making the transferred data inaccessible to said host computer.

Claims 55 – 58 (Cancelled)

Claim 59 (Currently Amended): The secure network of claim 25 wherein said network security controller includes means for sending updated user profiles to said security devices.

Claims 60 - 68 (Cancelled)

Claim 69 (Currently Amended): A method for controlling a sending computer to transmit information to a receiving computer over a computer network, the method comprising:

providing a security device at each sending computer and receiving computer;
setting user identification information at each security device for enabling a user to access the computer associated with the security device;

setting a plurality of user profiles at one or more of the security devices to enable a user, based on a user's user identifier, to select one of said plurality of user profiles, each user profile defining one or more destinations that the user is authorized to communicate with;

providing a network security controller on said computer network for receiving from said security device the identification of an authorized user identifier and the selected user profile and for forwarding the selected user profile to the security device for said authorized user identifier, including providing discretionary access control and mandatory access control policies for each user profile;

receiving information to be transmitted from the sending computer to the receiving computer at the sending computer security device;

implementing security mechanisms at a network layer of ISO protocol hierarchy to determine whether communication is authorized from the sending computer to the receiving computer by determining if the receiving computer is in a transmit list and consistent with a transmit security window through discretionary access control and mandatory access control, respectively and, if either condition is not satisfied then terminating the transmission of information and sending termination notice to the network security controller, otherwise encrypting the information to be transmitted; and

transmitting the encrypted information to the security device of the receiving computer over the computer network.

Claim 70 (Previously Amended): The method of claim 69 further comprising the step of changing user profiles at the network security controller and updating available user profiles at a security device.

Claim 71 (Previously Amended): The method of claim 69 further comprising the step of auditing the termination of transmission of information at the network security controller.

Claim 72 (Cancelled)

Claim 73 (Previously Amended): The method of claim 69 wherein said computer network includes the Internet.

Claim 74 (Previously Amended): The method of claim 69 wherein each security device prevents simultaneous connection at different security levels established by mandatory access controls.

Claim 75 (Previously Amended): The method of claim 69 wherein each security device prevents simultaneous connection to trusted and untrusted networks.

Claims 76 – 84 (Cancelled)

Claim 85 (Currently Presented): The network of claim 25 wherein said security devices include means for enabling a plurality of user profiles to be set for a single user identifier.

Claim 86 (Currently Amended): The network of claim 85 wherein said plurality of user profiles to be set for a single user identifier is specific to a particular host computer associated with the security device.

Claim 87 (Previously Amended): The network of claim 85 wherein at least one of said plurality of user profiles enables access to a plurality of destinations.

Claim 88 (Previously Amended): The network of claim 54 wherein at least one of said plurality of user profiles includes a plurality of destinations.

Claim 89 (Currently Amended): The network of claim 88 wherein said network security controller enables the security officer to generate different user profiles at different security devices for a single user identifier.